

# Referentiearchitectuur ProductDienstStatus

## **VNG Realisatie**

Nassaulaan 12  
2514 JS Den Haag

2021

# Inhoud

1.	Inleiding .....	3
1.1.	Versiebeheer .....	3
1.2.	Deelnemende organisaties .....	4
1.3.	Leeswijzer .....	4
2.	ProductDienstStatus .....	5
2.1.	Wat heeft de burger er aan? .....	5
2.2.	Wat hebben de overheidsorganisaties er aan? .....	5
3.	Bedrijfsarchitectuur.....	6
3.1.	Actoren en rollen .....	6
3.2.	Bedrijfsobjecten.....	7
3.3.	Bedrijfsprocessen en -diensten.....	8
4.	Informatiearchitectuur .....	14
4.1.	Interactiepatronen opvragen status .....	15
5.	Informatiebeveiliging en privacy.....	24
5.1.	Uitgangspunten .....	24
5.2.	Grootste risico's van PDS .....	24
5.3.	Maatregelen en componenten .....	25
5.4.	Verwerkingsregister en verwerkingenlogging .....	25
6.	Kaders en context .....	28
6.1.	Wet- en regelgeving .....	28
6.2.	Bouwblokken digitale overheid.....	31
7.	Principes.....	33
7.1.	Architectuurprincipes PDS .....	33
8.	Bijlagen.....	36
8.1.	Overzicht generieke PDS componenten .....	36
8.2.	Casus MijnGemeente.....	38
8.3.	Casus CRM .....	39
8.4.	Statusuitwisseling tussen organisaties .....	40

# 1. Inleiding

**Burgers, ondernemers en instellingen die contact hebben met de overheid doen dit via meer interactiekanalen. Denk aan het raadplegen van informatie via een website, mobiele app, online formulieren of een persoonlijk gesprek aan de balie. Die veelheid aan kanalen heeft voordelen: gericht een bepaald kanaal inzetten voor een bepaalde dienst voor een bepaalde doelgroep. Daarmee wordt het contact effectiever en efficiënter. Tegelijkertijd zijn er uitdagingen. Zo kunnen burgers het gevoel krijgen ‘van het kastje naar de muur te worden gestuurd’ door de complexiteit en diversiteit van kanalen. Met de omnichannel aanpak is dit te voorkomen.<sup>1</sup>**

Dit document beschrijft de referentiearchitectuur voor ProductDienstStatus (PDS) en is onderdeel van de referentiearchitectuur Omnichannel. De referentiearchitectuur PDS moet een solide basis vormen om de komende jaren informatievoorzieningen te ontwikkelen en te implementeren die niet alleen bijdragen aan een betere dienstverlening aan burgers, ondernemers en instellingen maar ook ambtenaren zo optimaal mogelijk ondersteunt in die dienstverlening.

De referentiearchitectuur PDS is in samenwerking met een aantal overheidsorganisaties uitgewerkt. De betrokkenheid van andere overheidsorganisaties naast gemeenten is van groot belang. Binnen één organisatie gegevens op gestandaardde wijze delen neemt maar een deel van het ‘kastje naar de muur’-gevoel weg bij een burger. Maar als diezelfde gegevensverstrekking ook tussen verschillende overheidsorganisaties gestandaardiseerd is, ontstaat de mogelijkheid echt als één overheid op te treden. Organisaties kunnen immers (binnen de kaders van de wet- en regelgeving) gegevens van de andere organisatie direct aan de burger tonen, zonder dat de burger daarvoor naar een apart loket of ander kanaal moet worden doorgestuurd. Om dit doel te bereiken willen we deze referentiearchitectuur PDS verder ontwikkelen en beproeven met overheidsorganisaties uit verschillende bestuurslagen.

## 1.1. Versiebeheer

Dit document is in beheer bij VNG-Realisatie.

Versie	Toelichting	Datum	Auteur(s)
0.1	Initiële opzet en ter review aangeboden aan innovatiegroep	1-10-2021	I. Hendriks / P. Jansen
0.2	Review verwerkt, aangevuld en ter review aangeboden	2-11-2021	I. Hendriks / P. Jansen
0.3	Review verwerkt, aangevuld en ter review aangeboden	12-11-2021	I. Hendriks / P. Jansen
0.9	Review verwerkt en opgeleverd t.b.v. Inspiratiedag Omnichannel	18-11-2021	I. Hendriks / P. Jansen

<sup>1</sup> <https://www.vngrealisatie.nl/producten/omnichannel-dienstverlening>

## 1.2. Deelnemende organisaties

Deze referentiearchitectuur is tot stand gekomen in samenwerking met onderstaande organisaties. De deelnemende organisaties hebben de conceptversies van review voorzien en hebben waardevolle input geleverd.

Dhr. H. van Hees	(gemeente Tilburg)
Dhr. M. Groenestein	(gemeente Helmond)
Dhr. R. Meijer	(gemeente Ooststellingwerf, Weststellingwerf en Opsterland)
Dhr. V. van Beek	(gemeente Den Haag)
Dhr. J. Verbeek	(gemeente Den Haag)
Dhr. J. Zwart	(Raad voor de Kinderbescherming)
Dhr. R. Sjouwerman	(Divosa)
Dhr. L. Vermeer	(ICTU)

## 1.3. Leeswijzer

Dit document is bedoeld voor architecten of informatiemanagers bij overheidsorganisaties die op basis van de referentiearchitectuur een eigen PDS-implementatie willen voorbereiden.

- Hoofdstuk 2 beschrijft in het kort wat ProductDienstStatus inhoudt;
- Hoofdstuk 3 beschrijft de Bedrijfsarchitectuur waarin de actoren, rollen en bedrijfsobjecten opgenomen zijn;
- Hoofdstuk 4 beschrijft de Informatiearchitectuur waarin referentiecomponenten in samenhang en in relatie met elkaar worden getoond;
- Hoofdstuk 5 beschrijft de Informatiebeveiliging en Privacy waaraan gedacht moet worden bij het toepassen van de referentiearchitectuur;
- Hoofdstuk 6 beschrijft de kader en context waaraan de architectuur moet voldoen;
- Hoofdstuk 7 beschrijft de principes die vanuit de referentiearchitectuur meegegeven worden;
- Hoofdstuk 8 beschrijft de gebruikte casussen om deze referentiearchitectuur vorm te geven.

## 2. ProductDienstStatus

**Burgers en ondernemers hebben vaak contact met de overheid. Dit contact verloopt via steeds meer interactiekanalen. Veel van deze contacten gaan over de levering van een product of dienst door de overheid aan een burger of ondernemer.**

Commerciële partijen als PostNL en Bol.com hebben de afgelopen jaren geoptimaliseerde klantportalen en ‘track & trace’-functionaliteit ontwikkeld waarmee bestellingen op ieder moment te volgen zijn. De overheid is op dit gebied minder ver. Reden om de referentiearchitectuur Omnichannel te verdiepen met een referentiearchitectuur ‘ProductDienstStatus’ (PDS). PDS is een publieke variant op ‘track & trace’, aansluitend bij publieke waarden, en voldoende aan wet en regelgeving die voor de overheid geldt.

“PDS omvat die informatie over de levering van producten en diensten door de overheid die voor burgers en bedrijven belangrijk is. Deze informatie wordt door de overheid proactief en via een kanaal naar keuze aan burgers en bedrijven aangeboden. PDS werkt ketenbreed en uniform: burgers en bedrijven worden op eenduidige wijze geïnformeerd, ook als bij de levering van een product of dienst meerdere (overheids)organisaties betrokken zijn.”

### 2.1. Wat heeft de burger er aan?

Burgers, bedrijven of instellingen die producten van de overheid afnemen, weten vaak niet (goed genoeg) wat de status van hun productaanvraag is of hoe lang het nog gaat duren voordat het product geleverd wordt. Het komt voor dat ze met meerdere organisaties contact moeten opnemen om dit te achterhalen – het bekende van het kastje naar de muur sturen. Met PDS kunnen burgers en bedrijven de levering van producten en diensten volgen, ook als daarbij meerdere (overheids)organisaties betrokken zijn. Zij worden proactief en via een kanaal naar keuze geïnformeerd over die levering, onder voorbehoud dat het kanaal door de organisatie beschikbaar is gesteld.

### 2.2. Wat hebben de overheidsorganisaties er aan?

Maar PDS helpt ook overheden: een goed geïnformeerde burger staat minder vaak aan de balie of maakt minder vaak contact middels een ander kanaal. En doordat overheidsorganisaties op een eenduidige manier informatie met elkaar delen, kunnen vragen worden beantwoord door een klantenservicemedewerker in plaats van de vakspecialist. Zij hebben daardoor meer tijd voor het leveren van goede dienstverlening en ondersteuning op maat. PDS-informatie kan daarnaast worden gebruikt voor het bewaken van het verloop van (keten)processen en het bijsturen van de inrichting daarvan.

## 3. Bedrijfsarchitectuur

Dit hoofdstuk beschrijft de actoren, bedrijfsobjecten en -processen en -diensten die bij het verstrekken en ontvangen van ProductDienstStatus (PDS)-informatie een rol spelen.

### 3.1. Actoren en rollen

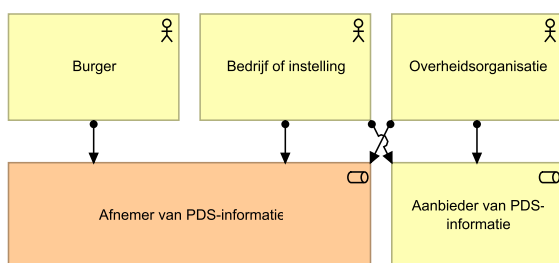
Bij het verstrekken en ontvangen van PDS-informatie kunnen drie actoren betrokken zijn.

- **Burger:** Iedere natuurlijke persoon die ingezetene is in Nederland (zoals opgenomen in de BRP), of is opgenomen in het Register Niet-Ingezetenen RNI.
- **Private partij:** een organisatie met of zonder winstoogmerk die tot doel heeft goederen en/of diensten te produceren en/of die te leveren aan andere organisaties of individuen.
- **Overheidsorganisatie:** een organisatie van de overheid die overheidstaken uitvoert of in opdracht van de overheid een wettelijke taak vervult (zoals zelfstandige bestuursorganen).

Bovengenoemde actoren kunnen drie rollen vervullen:

- **Afnemer van PDS-informatie:** degene die PDS-informatie gebruikt om inzicht te krijgen in de status van levering van een product of dienst. Dit kan zowel de indiener van een productaanvraag zijn, als een medewerker van een overheidsorganisatie
- **Aanbieder van PDS-informatie:** degene die handelingen uitvoert die ervoor zorgen dat de status van levering van een product of dienst verandert.

De relaties in Figuur 1 hieronder laten zien dat een burger alleen kan optreden als afnemer van PDS-informatie. Private partijen en overheidsorganisaties kunnen zowel de rol van afnemer als de rol van aanbieder daarvan vervullen.

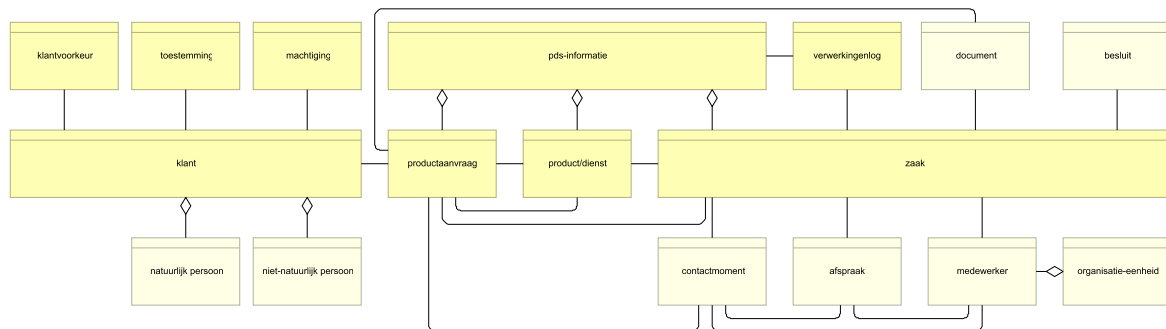


Figuur 1: Actoren en rollen betrokken bij het verstrekken en ontvangen van PDS-informatie.

### 3.2. Bedrijfsobjecten

Bij het verstrekken van PDS-informatie is een aantal bedrijfsobjecten betrokken. Deze kunnen verdeeld worden in drie categorieën:

1. Bedrijfsobjecten die informatie omvatten waaruit PDS-informatie is opgebouwd. Dit geldt voor 'productaanvraag', 'product/dienst' en 'zaak'. In Figuur 2 is deze relatie geïllustreerd door een aggregatierelatie tussen deze objecten en 'PDS-informatie'. Dit betekent dat PDS-informatie geen *nieuwe* informatie is, maar informatie die al binnen de overheidsorganisatie beschikbaar is, zoals aanvraag- en zaakstatussen, en statusbeschrijvingen en servicetermijnen die in een producten- en dienstencatalogus of zaaktypecatalogus beschreven zijn.
2. Bedrijfsobjecten die informatie omvatten die bepaalt of, en zo ja hoe PDS-informatie geleverd wordt. Het gaat dan bijvoorbeeld om klantvoorkeuren die bepalen welk kanaal voor levering van PDS-informatie wordt gebruikt, en toestemming die bepaalt of, en zo ja in welke mate een medewerker die daarvoor geen andere grondslag heeft toegang heeft tot statusinformatie bij aanvragen van een inwoner of bedrijf. Deze objecten zijn Figuur 2 donkergeel gekleurd.
3. Bedrijfsobjecten die een rol spelen tijdens het proces van aanvragen en leveren van producten en diensten, de referentiearchitectuur Omnichannel, en/of onderdeel uitmaken van een integraal klantbeeld, maar die bij het verstrekken van PDS-informatie een secundaire, of überhaupt geen rol spelen. Deze objecten zijn in Figuur 2 lichtgeel gekleurd.



*Figuur 2: Bedrijfsobjecten betrokken bij het verstrekken en ontvangen van PDS-informatie*

In de tabel hieronder zijn de definities voor de geïllustreerde bedrijfsobjecten opgenomen. Deze zijn voor zover daarin beschreven overgenomen uit de referentiearchitectuur Omnichannel of GEMMA-referentiearchitectuur.<sup>2</sup>

Bedrijfsobject	GEMMA-definitie
klantvoorkeur	De voorkeur die een klant heeft met betrekking tot de dienstverlening. Dit kan bijvoorbeeld gaan over het gewenste communicatiekanaal of een taalinstelling.
toestemming	De toestemming die een klant gegeven heeft aan een gemeente om klantgegevens in te zien of te verwerken.

<sup>2</sup> [https://www.gemmaonline.nl/index.php/GEMMA\\_Verbinding\\_bedrijfsfuncties\\_en\\_bedrijfsobjecten](https://www.gemmaonline.nl/index.php/GEMMA_Verbinding_bedrijfsfuncties_en_bedrijfsobjecten)



Bedrijfsobject	GEMMA-definitie
machtiging	De machtiging die een klant aan een ander natuurlijk persoon heeft verstrekt.
klant	Een natuurlijk persoon of niet-natuurlijk persoon waar een product/dienst wordt geleverd.
natuurlijk persoon	Een mens.
niet-natuurlijk persoon	Een rechtspersoon of een samenwerkingsverband.
productaanvraag	Een vraag of aanvraag voor een product/dienst door een klant.
product/dienst	Een tastbaar goed of verzameling activiteiten die door de gemeente geleverd kunnen worden.
contactmoment	Een aaneengesloten interactie tussen inwoner of (vertegenwoordiger van) een onderneming en de gemeente via een synchroon kanaal (telefoon, gesprek aan de balie) of een informatieverstrekking door de inwoner of (vertegenwoordiger van) een onderneming aan de gemeente of vice versa via een asynchroon kanaal (e-mail, contactformulier, chatbot) waarvan de inhoud relevant is voor de dienstverlening door de gemeente.
afpraak	Een gepland klantcontact tussen een klant en de gemeente.
medewerker	Een [natuurlijk persoon] met een tijdelijk of vaste [dienstbetrekking] of met een inhuurcontract met de gemeente.
organisatie-eenheid	Een clustering van medewerkers binnen de lijnorganisatie met een duidelijk gedefinieerde specifieke taakstelling.
zaak	Een samenhangende hoeveelheid werk met gedefinieerde aanleiding en een gedefinieerd eindresultaat waarvan kwaliteit en doorlooptijd bewaakt moeten worden.
pds-informatie	Informatie die inzicht geeft in het proces voor levering van een product of dienst, de huidige status van een specifieke productaanvraag binnen dat proces en een indicatie van de verwachte resterende levertijd.
document	Een informatieobject met als generieke aanduiding 'document' kan van alles zijn, ongeacht aard en vorm: een tekstverwerkingsdocument, een papieren brief, een webpagina, een landkaart, een foto, een geluidsopname, een dataset, een blog, etc.
besluit	Een beslissing over het wel of niet toekennen van [product/dienst].
verwerkingenlog	De vastlegging van een verwerking in een logregistratie om de verwerking van objectgegevens te kunnen duiden.

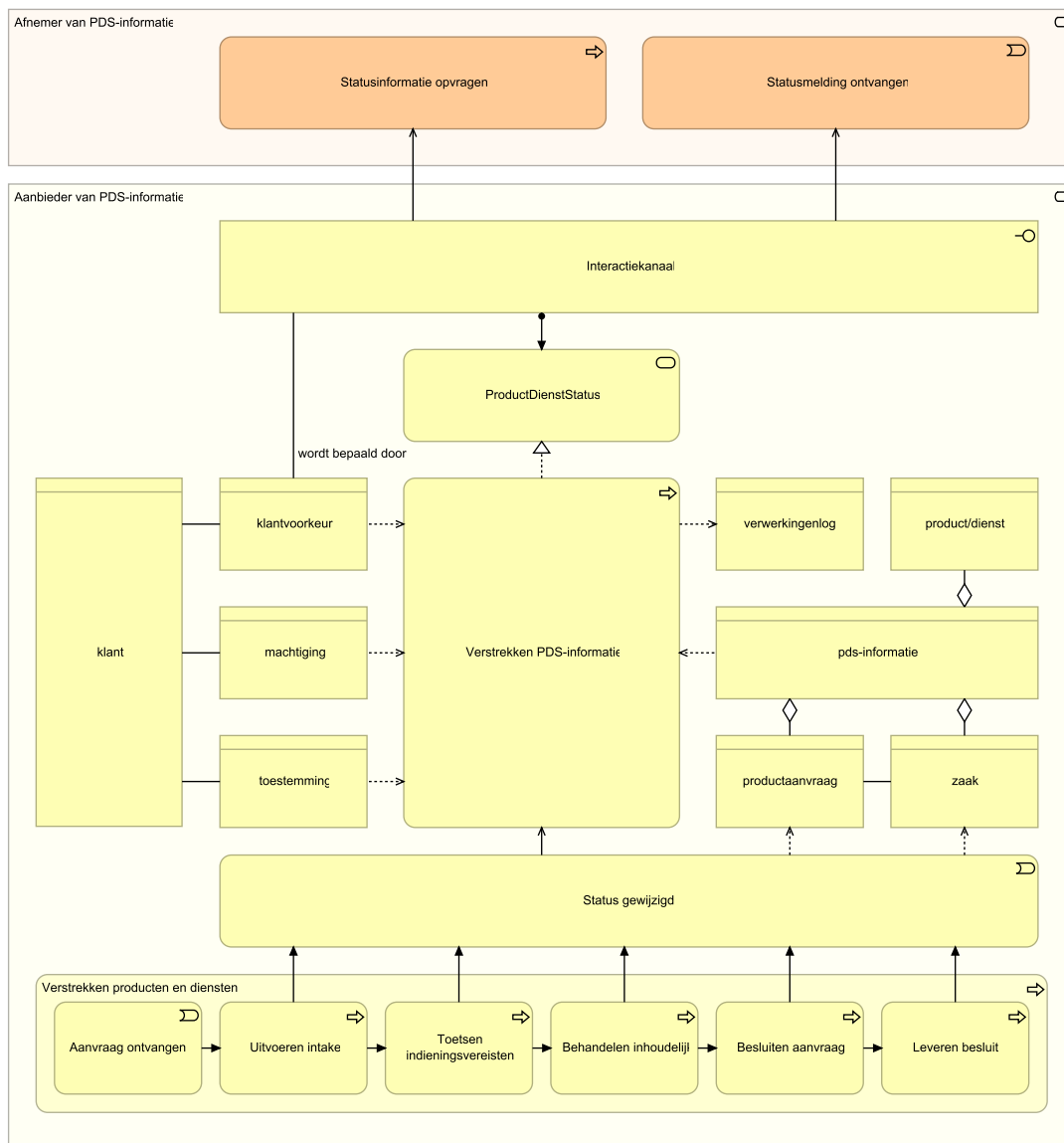
### 3.3. Bedrijfsprocessen en -diensten

Figuur 3 laat zien hoe PDS-informatie wordt verstrekt. De basis hiervoor is het bedrijfsproces 'Verstrekken van producten en diensten' dat de overheidsorganisatie naar aanleiding van een aanvraag voor een product of dienst door een burger of bedrijf of instelling is gestart. Deze aanvraag wordt zaakgericht behandeld. Tijdens de behandeling doorloopt de zaak verschillende fases. Hierbij ontstaan statuswijzigingen. Deze statuswijzigingen vormen de basis voor PDS-informatie.

Het leveren van PDS-informatie kent een eigen bedrijfsproces: 'Verstrekken PDS-informatie'. Tijdens het doorlopen van dit proces worden een aantal bedrijfsobjecten gelezen: 'klantvoorkeur' om PDS-informatie te kunnen leveren via het voorkeurskanaal van de klant, en 'machtigingen' en 'toestemmingen' om te bepalen of de afnemer wel recht heeft op inzage in de te verstrekken

gegevens. Daarnaast de uit 'productaanvraag', 'zaak'- en 'product/dienst'-informatie samengestelde PDS-informatie die aan de aanvrager verstrekt wordt. Het verstrekken van deze informatie wordt bovendien vastgelegd in een verwerkingenlog.

Interactie tussen de PDS-afnemer en aanbieder vindt plaats via de dienst 'ProductDienstStatus' die de PDS-aanbieder levert. Deze dienst kan worden aangeroepen via een daartoe door de PDS-aanbieder ingericht 'Interactiekanaal'. Dit kanaal ondersteunt zowel het opvragen van statusinformatie door een PDS-afnemer (pull-scenario, zie ook Figuur 5) als het ontvangen van statusinformatie op initiatief van de aanbieder verstrekte PDS-informatie (push-scenario, zie ook Figuur 4).



*Figuur 3: Generieke illustratie van bedrijfsprocessen en -diensten die een rol spelen bij de verstrekking van PDS-informatie*

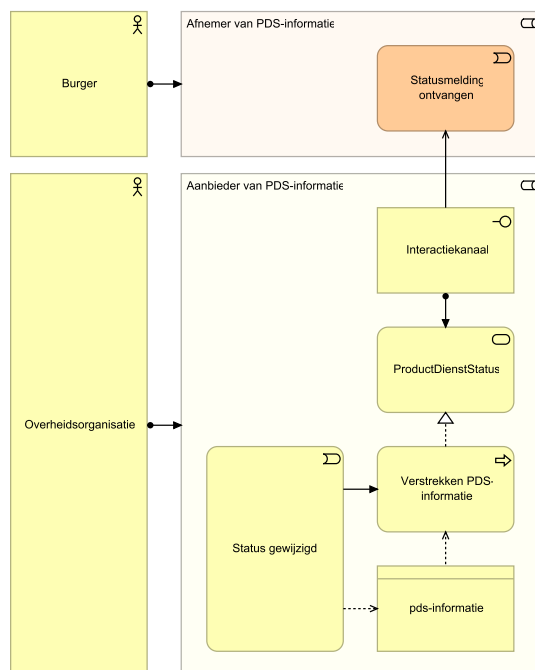
### 3.3.1. Scenario's voor levering van PDS-informatie

PDS-informatie kan op verschillende manieren aan afnemers geleverd worden. factoren die de wijze van leveren beïnvloeden zijn:

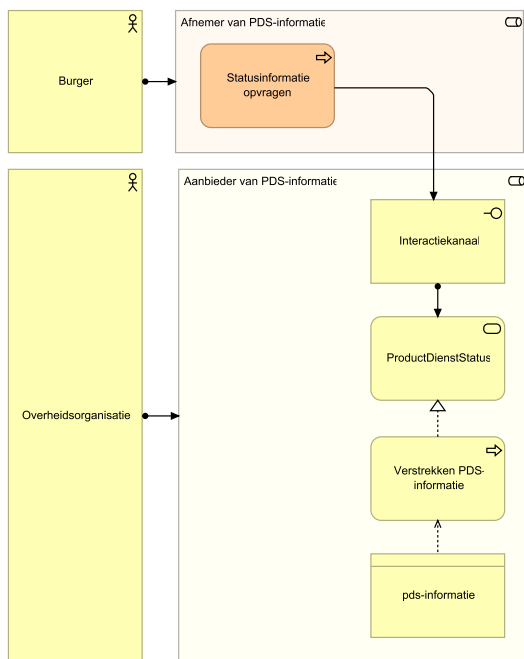
- **De aanleiding voor het leveren van PDS-informatie.** Een aanbieder van PDS-informatie kan een statusupdate naar een afnemer 'pushen' naar aanleiding van een veranderde status bij een aanvraag of zaak (Figuur 4), maar een (eind)afnemer kan ook het zelf het initiatief nemen tot het opvragen ('pullen') van de laatste statusinformatie (Figuur 5).
- **Het kanaal dat wordt gebruikt voor het opvragen van statusinformatie.** Een (eind)afnemer kan inzicht in statusinformatie krijgen via geautomatiseerde, digitale kanalen (Figuur 4, Figuur 5 en Figuur 7), of door te bellen naar het klantcontactcentrum van de overheidsorganisatie die de aanvraag behandelt (Figuur 6). In het laatste geval kan niet alleen de Burger, maar ook de KCC-medewerker van de Overheidsorganisatie waarmee contact wordt gelegd gezien worden als afnemer van PDS-informatie
- **De betrokkenheid van meerdere organisaties.** Als meerdere organisaties betrokken zijn bij de levering van een product of dienst aan een (eind)afnemer, dan geldt de overheidsorganisatie bij de wie de oorspronkelijke productaanvraag is ingediend niet alleen als aanbieder (aan de burger die geldt als (eind)afnemer)) van PDS-informatie, maar ook als afnemer van door de ketenpartner aangeleverde PDS-informatie (Figuur 7).

In onderstaande diagrammen treedt steeds een burger op als (eind)afnemer. Maar deze rol zou ook kunnen worden vervuld door een private partij of een (tweede) overheidsorganisatie.

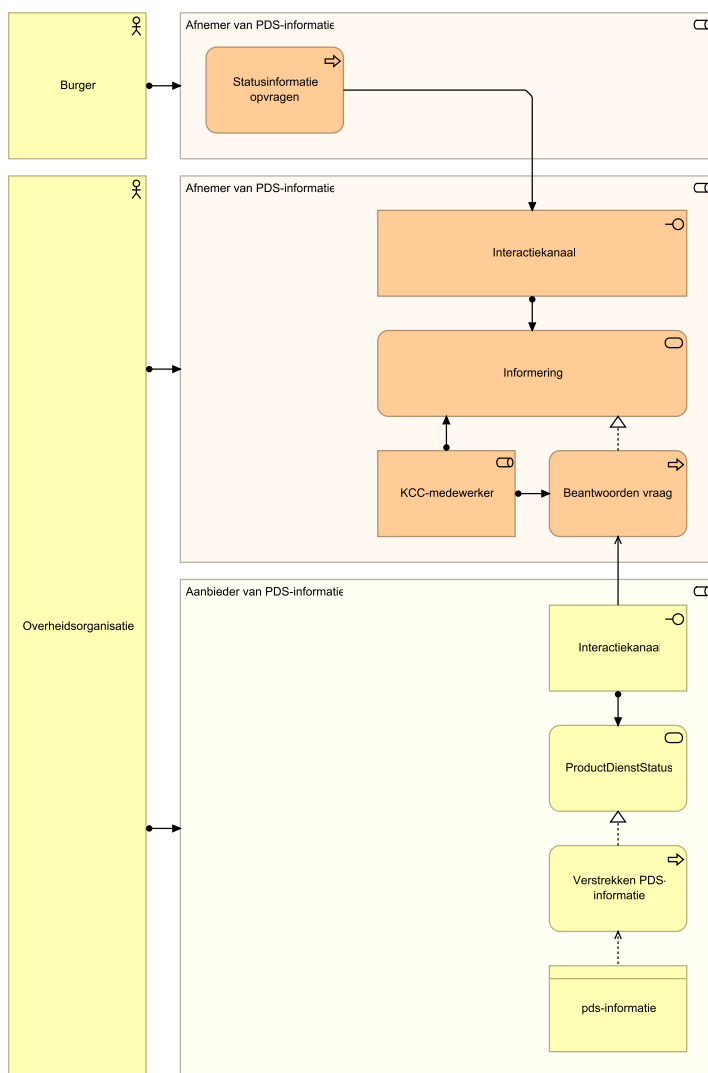
De diagrammen sluiten aan bij de in hoofdstuk 8 beschreven casussen. Figuur 5 bij 'MijnGemeente', Figuur 6 bij 'CRM' en Figuur 7 bij 'Statusuitwisseling tussen organisaties'.



Figuur 4: levering naar aanleiding van veranderde status



*Figuur 5: levering op aanvraag van burger (of andere (eind)afnemer)*



*Figuur 6: levering op initiatief van burger (of andere (eind)afnemer) via KCC van overheidsorganisatie*



## 4. Informatiearchitectuur

**Dit hoofdstuk beschrijft de informatiearchitectuur voor PDS. In de informatiearchitectuur worden interacties tussen relevante referentiecomponenten beschreven. Daarbij wordt ook een relatie gelegd naar de eerder besproken bedrijfsobjecten, -processen en -diensten om aan te geven welke informatie bij een interactie verwerkt wordt.**

De informatiearchitectuur volgt het 5-lagen model van het GEMMA Gegevenslandschap<sup>3</sup> en de informatiekundige visie Common Ground<sup>4</sup>. Elementen uit de bedrijfsarchitectuur worden buiten deze 5 lagen geplaatst.

### **Laag 5 – Interactie**

De componenten in deze laag verzorgen de interactie met de gebruikers. Voor de interactie met burgers kunnen dit websites, apps of chatbots zijn. Een medewerker van een organisatie maakt doorgaans gebruik van een interne (web)applicatie.

### **Laag 4 – Proceslogica**

Het verloop van interacties waarbij gegevens opgehaald of verwerkt worden in de achterliggende registers wordt vormgegeven in deze laag. Door de logica los te koppelen van de interactie ontstaat een onafhankelijkheid in het gebruik van een interface of kanaal. Bijvoorbeeld, het opvragen van een status via een website verloopt daardoor op dezelfde manier als via een chatkanaal.

### **Laag 3 – Integratie**

In deze laag bevinden zich de componenten die de dienstenafnemers (laag 4 en 5) verbinden met de dienstenaanbieders (laag 1 en 2). Denk hierbij aan een API-gateway of een Enterprise Service Bus. Omwille van de leesbaarheid van onderstaande diagrammen wordt deze laag niet gevuld met de benodigde componenten. De relaties tussen de proceslogica en de gebruikte diensten (API's) zouden wegvallen waardoor niet duidelijk is welke processtap welke gegevens verwerkt.

### **Laag 2 – Diensten**

Gegevens die verwerkt worden, worden ontsloten via API's. Er kunnen meerdere API's beschikbaar gesteld zijn voor het bewerken van gegevens. Bijvoorbeeld omdat dit vanwege de veiligheid beter te organiseren is. API's kunnen ook gecombineerd worden, zodat een soort convenience API ontstaat waarbij gegevens uit meerdere bronnen gecombineerd worden teruggegeven aan de afnemer. Op die manier wordt voorkomen dat teveel gegevens opgehaald en getoond worden aan de gebruiker.

### **Laag 1 – Gegevens**

De componenten bevatten de (bron)gegevens. Deze gegevens worden ontsloten via de bovenliggende API's.

---

<sup>3</sup> <https://www.gemmaonline.nl/index.php/Gegevenslandschap>

<sup>4</sup> [https://www.gemmaonline.nl/index.php/Common\\_Ground](https://www.gemmaonline.nl/index.php/Common_Ground)

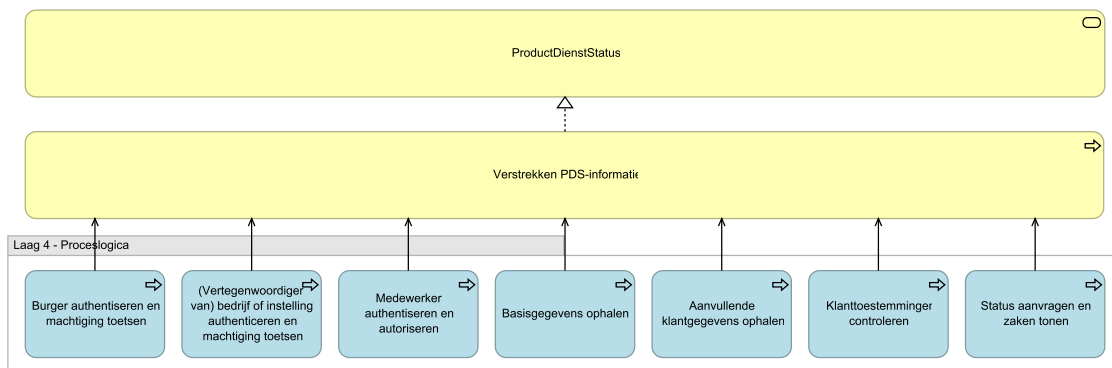
## 4.1. Interactiepatronen opvragen status

Deze paragraaf beschrijft hoe PDS-informatie uit (bron)registraties wordt opgehaald en hoe voor verschillende doelgroepen en situaties kan worden voldaan aan voorwaarden (authenticatie, autorisatie, controleren machtigingen en toestemmingen) om die te mogen leveren.

### 4.1.1. Verbinding met de bedrijfsarchitectuur

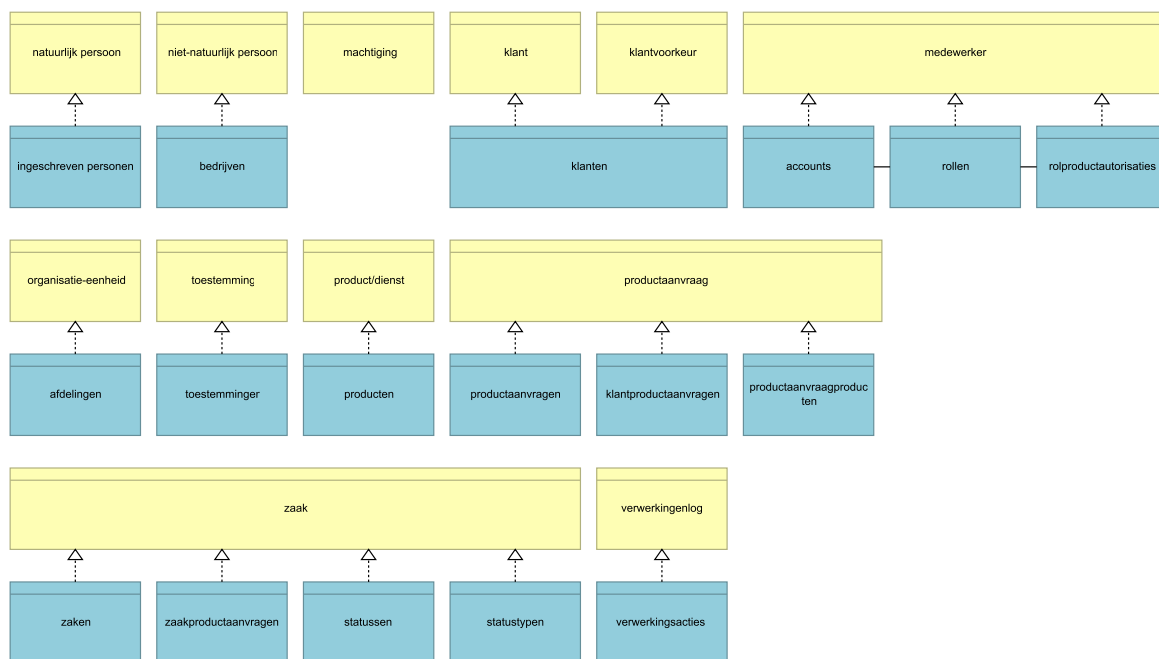
In hoofdstuk 3 is de bedrijfsarchitectuur voor ProductDienstStatus beschreven. In deze paragraaf beschrijven we als onderdeel van de informatiearchitectuur interactiepatronen. Deze hangen op twee manieren samen met de bedrijfsarchitectuur.

1. De verschillende applicatieprocessen die de hieronder beschreven interactiepatronen ondersteunen samen het in het vorige hoofdstuk beschreven bedrijfsproces 'Verstrekken PDS-informatie en de bedrijfsdienst 'ProductDienstStatus' (Figuur 8).
2. Gegevensobjecten die in de hieronder beschreven interactiepatronen worden geraadpleegd of gewijzigd realiseren volgens de in Figuur 9 geïllustreerde structuur de in Figuur 2 beschreven bedrijfsobjecten.



*Figuur 8: relatie tussen bedrijfsproces 'Verstrekken PDS-informatie' en bedrijfsdienst 'ProductDienstStatus' en applicatieprocessen uit interactiediagrammen*





*Figuur 9: relatie tussen bedrijfsobjecten en in interactiediagrammen geraadpleegde of gewijzigde gegevensobjecten*

Het hieronder beschreven interactiepatroon illustreert hoe informatie over de status van een aanvraag van een product of dienst aan een burger of medewerker wordt getoond. Zichtbaar wordt welke gegevensobjecten hiervoor nodig zijn, en via welke gegevenscomponenten en API-interfaces die beschikbaar worden gesteld.

Het patroon is beschreven in zes onderdelen:

1. **Burger authentifieren en machtigingen toetsen** – beschrijft op welke manier de identiteit van een burger wordt gecontroleerd en diens machtigingen getoetst. Van de drie in de bijlagen beschreven casussen is dit deel alleen relevant voor de casus 'MijnGemeente'.
2. **Bedrijf of instelling authentifieren en machtigingen toetsen** – beschrijft op welke manier de identiteit van een vertegenwoordiger van een bedrijf of instelling wordt vastgesteld en diens machtigingen om namens bedrijf of instelling te handelen worden opgehaald en gecontroleerd. Van de drie in de bijlagen beschreven casussen is dit deel alleen relevant voor de casus 'MijnGemeente'.
3. **Medewerker authentifieren en autoriseren en klanttoestemmingen controleren** – beschrijft op welke manier de identiteit van een medewerker wordt vastgesteld, diens autorisaties worden opgehaald. Van de drie in de bijlagen beschreven casussen is dit deel alleen relevant voor de casus 'CRM'.
4. **Klantgegevens ophalen** – beschrijft hoe contactgegevens en klantvoorkeuren (bijvoorbeeld een voorkeurskanaal) worden opgehaald.
5. **Klanttoestemmingen controleren** – beschrijft hoe wordt gecontroleerd of een afnemer toestemming heeft gegeven voor verwerking van (persoons)gegevens in het kader van verstrekking van PDS-informatie (dit voor zover het gaat om gegevens die niet op basis van een andere grondslag mogen worden verwerkt).

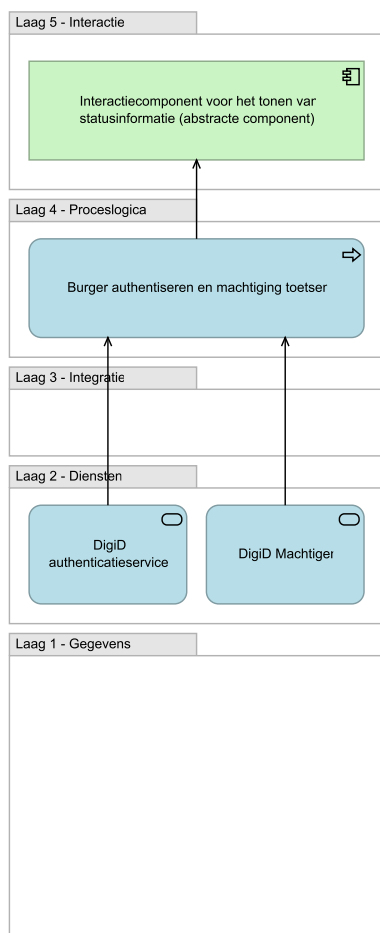
6. **Status lopende aanvragen en zaken tonen** – beschrijft op welke manier statusinformatie over de aanvraag van een product of dienst aan een burger, medewerker óf andere organisatie worden getoond. Dit deel van het interactiepatroon dus generiek en geldend voor alle casussen waarbinnen PDS-informatie wordt geleverd.

Niet ieder van de bovengenoemde onderdelen is in iedere situatie nodig. Zo hoeft afhankelijk van de doelgroep (burgers, bedrijven en organisaties of medewerkers) waartoe de afnemer behoort maximaal eenmaal een autorisatie- en authenticatieproces doorlopen te worden. Maar in gevallen waar ‘openbare’ gegevens als PDS-informatie worden geleverd (bijvoorbeeld statusinformatie naar aanleiding van een melding over een defecte lantaarnpaal) kunnen authenticatie en autorisatie wellicht überhaupt achterwege blijven.

Een ander voorbeeld is het controleren van toestemmingen. Als een afnemer zelf het initiatief neemt voor het inzien van PDS-informatie hoeft niet door de aanbieder gecontroleerd te worden of hij of zij toestemming heeft gegeven voor het verwerken van persoonlijke gegevens voor dat doel – het initiatief is dan immers de toestemming. Als een overheidsorganisatie aan de andere kant een afnemer geautomatiseerd van iedere statuswijziging op de hoogte wil stellen is zo’n controle weer wel nodig.

Een overzicht van generieke componenten en API’s die betrokken (kunnen) zijn bij het ontstaan of tonen van PDS-informatie is te vinden in bijlage 8.1.

#### 4.1.2. Burger authenticiseren en machtigen toetsen

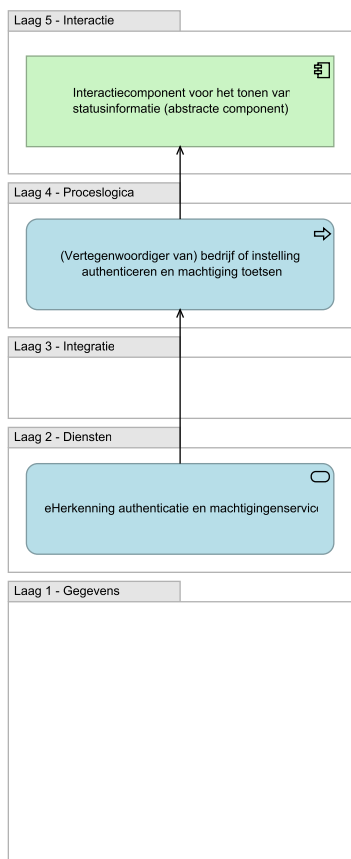


*Figuur 10: Interactiediagram 'burger authenticiseren en machtigen toetsen'*

Dit diagram omvat twee applicatieproces:

Applicatieproces	Beschrijving
Burger authenticiseren en machtigen toetsen	De identiteit van de burger wordt vastgesteld middels een authenticatiemiddel met een betrouwbaarheid die aansluit bij de gevoeligheid van de als PDS-informatie te leveren gegevens. Daarnaast wordt gecontroleerd welke machtigen de burger heeft om producten aan te vragen namens iemand anders (bijvoorbeeld omdat die burger optreedt als bewindvoerder voor een andere burger) of welke machtigen diegene heeft om PDS-informatie namens iemand anders op te vragen.

#### 4.1.3. (Vertegenwoordiger van) bedrijf of instelling authenticiseren en machtigingen toetsen

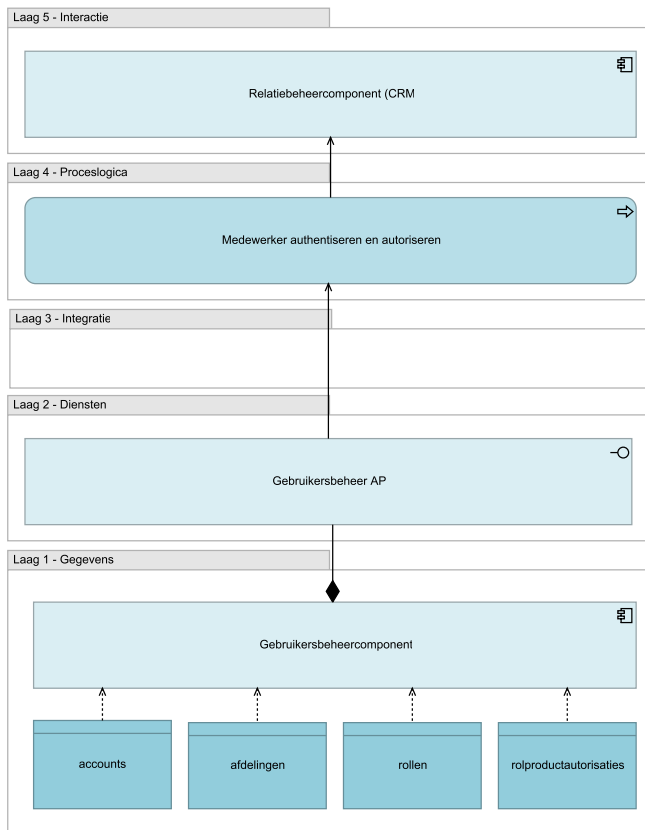


*Figuur 11: Interactediatom ' (Vertegenwoordiger van) bedrijf of instelling authenticiseren en machtigingen toetsen '*

Dit diagram omvat een applicatieproces:

Applicatieproces	Beschrijving
(Vertegenwoordiger van) bedrijf of instelling authenticiseren en machtigingen toetsen	De gebruiker wordt geauthentiseerd om vast te stellen dat die het recht heeft om het bedrijf of de instelling te vertegenwoordigen. Daarnaast wordt gecontroleerd welke machtigingen de gebruiker heeft om namens het bedrijf of de instelling te handelen.

#### 4.1.4. Medewerker authenticiseren en autoriseren

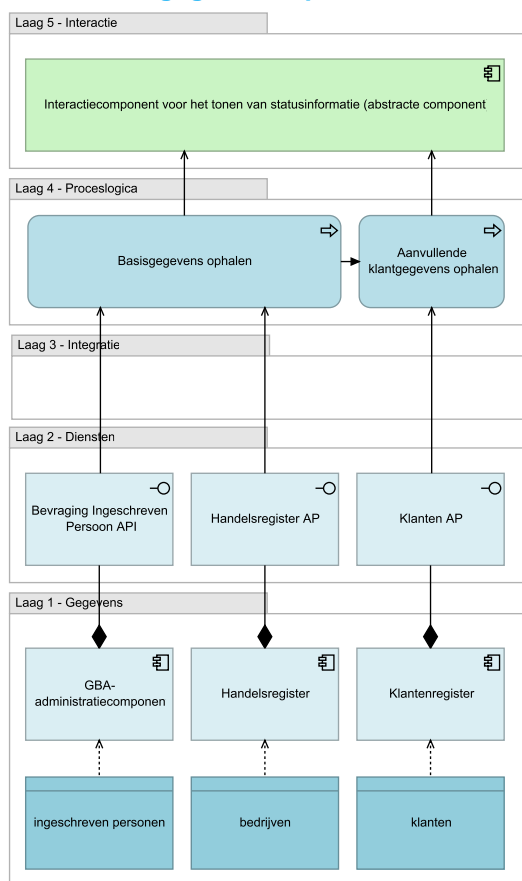


Figuur 12: Interactiediagram 'Medewerker authenticiseren en autoriseren'

Dit diagram omvat één applicatieproces:

Applicatieproces	Beschrijving
Medewerker authenticiseren en autoriseren	De identiteit van de medewerker wordt vastgesteld middels een authenticatiemiddel met een betrouwbaarheid die aansluit bij de gevoeligheid van de als PDS-informatie te leveren gegevens. Daarnaast worden de rollen waaraan de medewerker is toegewezen opgehaald. Aan de hand van autorisatieprofielen die gekoppeld zijn aan producten of diensten wordt vastgesteld of de medewerker - via de aan hem of haar toegewezen rollen - de juiste autorisaties bezit om toegang te krijgen tot de gevraagde PDS-informatie.

#### 4.1.5. Klantgegevens ophalen



Figuur 13: Interactiediagram 'Klantgegevens ophalen'

Dit diagram omvat twee applicatieprocessen:

Applicatieproces	Beschrijving
Basisgegevens ophalen	<p>Basisgegevens van de afnemer worden op basis van een uniek identificerend gegeven (afhankelijk van de doelgroep BSN, OIN of KvK-nummer) opgehaald. Daartoe wordt eerst de GBA-administratiecomponent (burger, BSN) of het Handelsregister (bedrijf of instelling, OIN of KvK-nummer) bevraagd.</p> <p><i>Deze stap is optioneel</i></p>
Klantgegevens ophalen	<p>Op basis van (een combinatie van) (zeer waarschijnlijk) uniek identificerend(e) gegeven(s) worden aanvullende klantgegevens en klantvoorkeuren (zoals voorkeurskanalen) opgehaald uit het Klantenregister. Het uniek identificerende gegeven kan een BSN, OIN of KvK-nummer uit de vorige stap zijn, maar ook bijvoorbeeld een combinatie van zaaknummer en naam of e-mailadres. Op basis van het laatste mogen slechts beperkt gevoelige gegevens worden verstrekt.</p>

#### 4.1.6. Klanttoestemmingen controleren

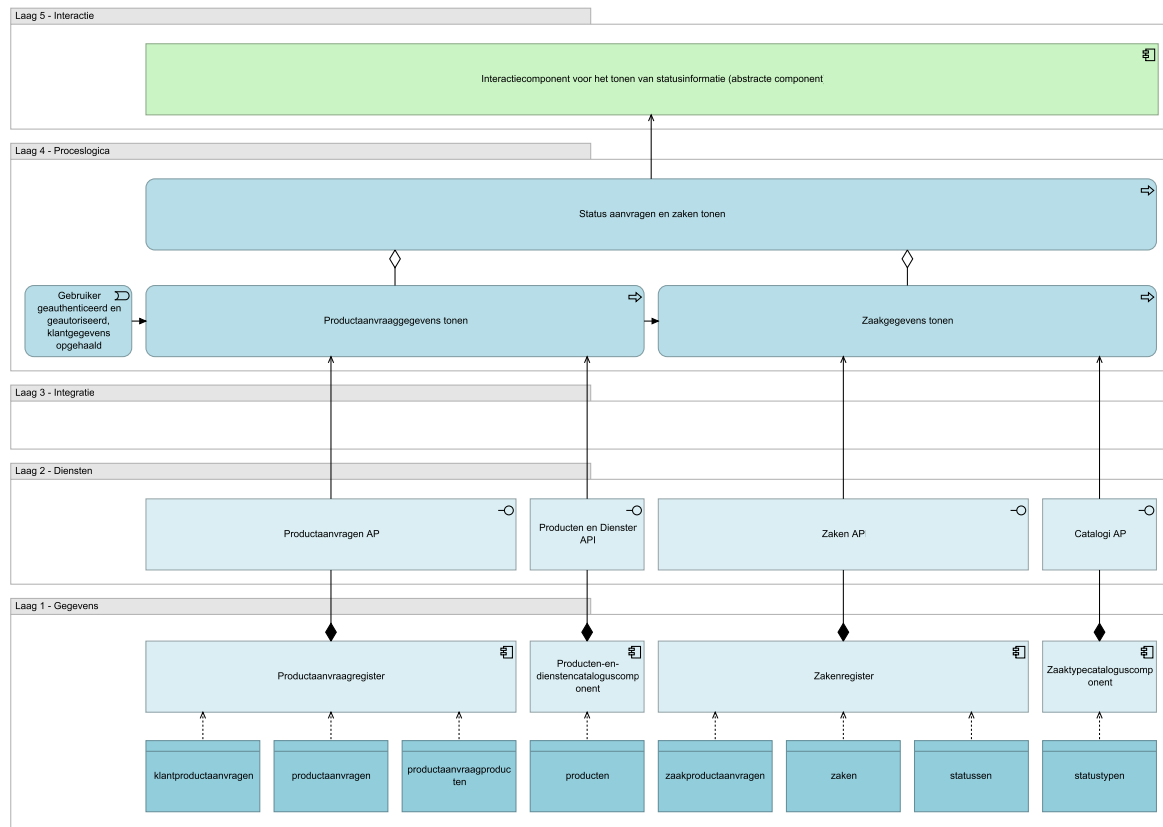


Figuur 14: Interacted diagram 'Klanttoestemmingen controleren'

Dit diagram omvat één applicatieproces:

Applicatieproces	Beschrijving
Klanttoestemmingen controleren	Er wordt gecontroleerd of, en zo ja in welke mate de afnemer toestemming heeft gegeven voor verwerking van (persoons)gegevens voor dit doel (dit voor zover het gaat om gegevens die niet op basis van een andere grondslag mogen worden verwerkt).

#### 4.1.7. Status lopende aanvragen en zaken tonen



Figuur 15: Interactiediagram 'Status lopende aanvragen en zaken tonen'

Dit diagram omvat drie applicatieprocessen:

Applicatieproces	Beschrijving
Status aanvragen en zaken tonen	Alle beschikbare informatie over de status van levering van een door een afnemer aangevraagd(e) product of dienst wordt opgehaald en getoond.
Productaanvraaggegevens tonen	Op basis van een relatie tussen klanten in het Klantenregister en via het gegevensobject klantproductaanvragen in het Productaanvragenregister worden de door de burger opgevraagde productaanvraaggegevens (o.a. moment van indienen en aangevraagd product) opgehaald en getoond. Op basis van een relatie met productaanvragen via het gegevensobject productaanvraagproducten in het Productaanvragenregister worden uit de Producten-en-dienstencataloguscomponent aanvullende gegevens over het aangevraagde product (zoals een beschrijving en behandeltermijnen) opgehaald en getoond.
Zaakgegevens tonen	Op basis van een relatie met productaanvragen via het gegevensobject zaakproductaanvragen in het Zakenregister worden de zaak- en statusgegevens van de za(a)k(en) die naar aanleiding van de ingediende productaanvraag zijn gestart opgehaald en getoond. Op basis van de relatie van statussen naar statustypen in de Zaaktypecataloguscomponent worden op basis van het gegevensobject statustypen aanvullende gegevens over statussen (zoals de omschrijving daarvan) opgehaald en getoond.



## 5. Informatiebeveiliging en privacy

**Informatiebeveiliging en privacy zijn binnen de referentiearchitectuur PDS belangrijke aandachtspunten. Daarbinnen worden immers (ook) gevoelige, persoonlijke gegevens verwerkt.**

De inhoud van dit hoofdstuk omvat enkele beveiligings- en privacyprincipes, maar is een eerste, theoretische uitwerking. Uiteindelijk moet op basis van pilots een meer gedetailleerde risicoanalyse worden gemaakt. Bij het maken van die nadere risicoanalyse zal gebruikgemaakt worden van de IRPA tool van de IBD zodat de analyses vastgelegd en te hergebruiken zijn door gemeenten die met PDS aan de slag gaan.

### 5.1. Uitgangspunten

De volgende uitgangspunten gelden in generieke zin bij de implementatie van PDS:

- Burgers, bedrijven of instellingen zien alleen ‘eigen’ gegevens of gegevens waarvoor zij gemachtigd zijn;
- De privacy van de medewerkers van organisaties moet gewaarborgd zijn;
- Medewerkers van organisaties verwerken alleen die gegevens waarmee een doelbinding is;
- Alleen de juiste gegevens worden verwerkt en getoond.

### 5.2. Grootste risico's van PDS

Op basis van hetgeen in deze referentiearchitectuur is beschreven, is een ruwe schatting te maken van dreigingen en risico's om rekening mee te houden. In willekeurige volgorde zijn dit:

- Er worden onjuiste gegevens verstrekt. Dit kunnen niet-integere gegevens (bronsysteem) zijn of door het gebruik van een verkeerde koppeling;
- Gegevens of informatie wordt aan verkeerde mensen verstrekt (burgers, ambtenaren en ketenpartijen). Bijvoorbeeld door onjuiste authenticatie of autorisatie;
- De informatiesystemen die de gegevens moeten verwerken/verstrekken zijn niet beschikbaar. Mogelijk raken dan andere kanalen overbelast;
- Er wordt te weinig informatie verstrekt waardoor alsnog aanvullende vragen worden gesteld;
- Er wordt teveel informatie verstrekt. Dit kan bijvoorbeeld gebeuren doordat:
  - In het kader van doelbinding teveel gegevens aan medewerkers worden getoond;
  - Informatie wordt niet goed gefilterd;
- In het geval van eHerkenning het niet kunnen loggen op persoon maar op organisatie, waardoor niet duidelijk is wie wat heeft ingezien;
- PDS is door middel van een API gateway vanaf het internet direct beschikbaar. Er bestaat een risico is dat derden toegang krijgen tot gegevens waar ze niet bij mogen.

### 5.3. Maatregelen en componenten

De volgende maatregelen kunnen of moeten genomen worden om de risico's weg te nemen of te minimaliseren:

- Autoriseren op zaakniveau / gegevens- en attribuutniveau / afnemer, onafhankelijk van kanaal;
- Zorgdragen dat op basis van autorisatie onderscheid kan worden gemaakt tussen inzage in "dat"- (inhoud) en "wat"- (procesverloop)-informatie;
- Er moeten beschikbaarheidsmaatregelen genomen worden zodat uitval van een informatiesysteem wordt beperkt;
- Er moet vastgelegd worden welke persoon welke gegevens op welk moment heeft ingezien;
- Het moet duidelijk gepubliceerd of gecommuniceerd zijn waar een burger, bedrijf of instelling terecht kan als er verstoringen bij het ophalen van gegevens worden geconstateerd;
- Veilig ontwikkelen/hanteren ontwikkelstandaarden;
- Tijdens en na het implementeren van (aanpassingen aan) de componenten worden testen uitgevoerd om de veiligheid en privacy te waarborgen (dit betreft ook pentesten);
- PDS is internet facing middels een API gateway, dit betekent dat maatregelen goed ingeregeld moet worden om geen afbreuk te doen aan beveiliging;
- Er is gedegen documentatie beschikbaar waarin is beschreven hoe de informatievoorziening is geïmplementeerd en welke beveiligings- en privacymaatregelen getroffen zijn;
- Voor iedere PDS-implementatie wordt een IRPA analyse uitgevoerd.

VNG Realisatie start eind 2021 met het uitwerken van een architectuur die beschrijft hoe IAM-functionaliiteit er in een gegevenslandschap uit moet zien. De hieruit voortkomende principes en architectuur gaan in op het veilig ontsluiten van gegevens via API's. Zodra deze uitwerking beschikbaar is, wordt een verwijzing hiernaar in deze referentiearchitectuur opgenomen.

### 5.4. Verwerkingsregister en verwerkingenlogging

Eén van de genoemde risico's is het verstrekken van teveel gegevens aan een medewerker. Dit kan gebeuren als niet duidelijk is met welke doelbinding de gegevens opgevraagd mogen worden. Organisaties zijn volgens Artikel 30 lid 1 AVG verplicht om een verwerkingsregister bij te houden. In een verwerkingsregister is o.a. vastgelegd:

- (1) uw naam en contactgegevens;
- (2) de naam en contactgegevens van partijen waarmee u gezamenlijke verwerkingsverantwoordelijke bent;
- (3) de contactgegevens van de functionaris voor gegevensbescherming (FG) ;
- de verwerkingsdoeleinden;
- de categorieën van betrokkenen en categorieën van persoonsgegevens;
- de categorieën van ontvangers;

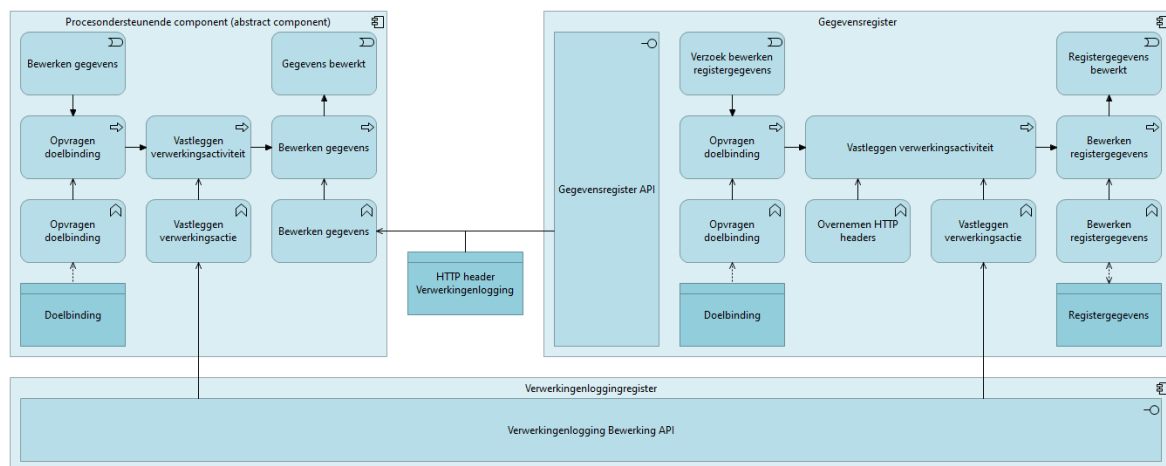
- eventuele doorgiften van persoonsgegevens aan derde land of internationale organisatie;
- indien mogelijk, de bewaartermijnen;
- indien mogelijk, de beveiligingsmaatregelen.

De Informatiebeveiligingsdienst (IBD) heeft een handreiking geschreven hoe om te gaan met deze verplichting<sup>5</sup>. Ook is er een voorgevuld verwerkingsregister beschikbaar gesteld<sup>6</sup>.

Een aanvullende maatregel hierop is het vastleggen van de verwerkingsacties die op persoonsgegevens zijn uitgevoerd. Elke component die persoonsgegevens afneemt of aanbiedt, moet deze verwerkingsactie vastleggen. Het vastleggen gebeurt in een verwerkingenloggingregister. Door VNG Realisatie is de Verwerkingenlogging API-standaard ontwikkeld als onderdeel van de GEMMA referentiearchitectuur. Deze API-standaard biedt leveranciers van informatiesystemen gestandaardiseerde API-specificaties voor het vastleggen en ontsluiten van de logging van verwerkingen<sup>7</sup>.

In deze referentiearchitectuur is daarom de referentiecomponent Verwerkingenloggingregister en bijhorende Verwerkingenlogging API opgenomen.

Onderstaande afbeeldingen zijn afkomstig uit de referentiearchitectuur Verwerkingenloggingregister en illustreren de relatie en afhankelijkheden tussen de relevante referentiecomponenten.<sup>8</sup>



Figuur 16: Interactiediagram waarbij een dienstenafnemer gegevens opvraagt bij een dienstenaanbieder

5

<https://www.informatiebeveiligingsdienst.nl/product/handreiking-verwerkingsregister-gemeenten-toelichting-bij-het-vooringevulde-register-van-verwerkingsactiviteiten/>

6 <https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/>

7 [https://www.gemmaonline.nl/index.php/Thema\\_Logging\\_en\\_verwerkingsactiviteiten](https://www.gemmaonline.nl/index.php/Thema_Logging_en_verwerkingsactiviteiten)

8 [https://www.gemmaonline.nl/index.php/Verwerkingenlogging\\_Interactiepatroon\\_Consumercomponenten\\_en\\_https://www.gemmaonline.nl/index.php/Verwerkingenlogging\\_Interactiepatroon\\_Consumer\\_Inzage](https://www.gemmaonline.nl/index.php/Verwerkingenlogging_Interactiepatroon_Consumercomponenten_en_https://www.gemmaonline.nl/index.php/Verwerkingenlogging_Interactiepatroon_Consumer_Inzage)



## 6. Kaders en context

### 6.1. Wet- en regelgeving

Nr.	Verplichting	Bron	Toelichting
1	Beperkt recht op inzage door burgers bij behandeling vertrouwelijke of gevoelige zaken <sup>9</sup>	Algemene Verordening Gegevensbescherming (AVG) en materie- wetgeving	Op basis van artikel 23 lid 1 onderdeel i van de AVG mag inzage door burgers in eigen persoonsgegevens geweigerd worden als die afbreuk zou doen aan 'rechten en vrijheden van anderen'. Bovendien kennen verschillende 'materiewetten' (bijvoorbeeld artikel 7.3.11 lid 3 Jeugdwet, artikel 5.3.2 lid 4 Wmo 2015) bepalingen op basis waarvan inzage in gevoelige informatie door betrokkenen geweigerd kan worden. Dit betekent dat aan burgers geen statusinformatie verstrekt wordt over bijvoorbeeld een onderzoek naar fraude of een onderzoek naar aanleiding van een melding bij Veilig Thuis.
2	Medewerkers hebben alleen toegang tot informatie die nodig is om een burger of ondernemer te helpen <sup>10</sup>	Algemene Verordening Gegevensbescherming (AVG)	Persoonsgegevens die worden verwerkt moeten toereikend en ter zake dienend zijn, en beperkt zijn tot wat noodzakelijk is voor de doeleinden. Daarbij gaat het om proportionaliteit en subsidiariteit, waardoor een minimum aan verwerking van persoonsgegevens wordt gerealiseerd (artikel 5, eerste lid, onder c, van de AVG). Er mogen niet meer gegevens dan nodig worden verwerkt en er moet goed worden bezien of het doel niet op een manier kan worden bereikt die minder inbreuk maakt op privacy.
3	Overheidsorganisaties moeten zich kunnen verantwoorden over verwerkte persoonsgegevens <sup>11</sup>	Algemene Verordening Gegevensbescherming (AVG)	Overheidsorganisaties moeten kunnen aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals rechtmatigheid, transparantie, doelbinding en juistheid. Ook moet aangetoond kunnen worden dat de juiste technische en organisatorische maatregelen genomen zijn om de persoonsgegevens te beveiligen.

<sup>9</sup> <https://www.schulinck.nl/app/uploads/Factsheet-privacy-sociaal-domein.pdf> en [https://www.divosa.nl/sites/default/files/bijeenkomst\\_bestanden/handreiking\\_privacy\\_in\\_het\\_sociaal\\_domein.pdf](https://www.divosa.nl/sites/default/files/bijeenkomst_bestanden/handreiking_privacy_in_het_sociaal_domein.pdf).

<sup>10</sup> <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken>.

<sup>11</sup> <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht>.

Nr.	Verplichting	Bron	Toelichting
4	Overheidsinformatie is duurzaam toegankelijk en wordt (indien van toepassing) op het aangewezen moment vernietigd <sup>12</sup>	Archiefwet	Overheidsorganisaties houden hun informatie ('archiefbescheiden') duurzaam toegankelijk, en/of die vernietigen die wanneer de bewaartermijn is verlopen. Dit is belangrijk omdat overheidsinformatie een rol speelt bij rechtsvinding en de (publieke) verantwoording door diezelfde overheid. Overheidsorganisaties moeten daarom aan burgers of derden verstrekte informatie archiveren, of die verstrekking op zodanige wijze vastleggen (loggen), dat onomstotelijk kan worden bewezen op welk moment aan wie welke gegevens geleverd zijn.
5	Verplicht aangewezen open standaarden worden gebruikt <sup>13</sup>	Wet digitale overheid (nog niet in werking)	Overheidsorganisaties kunnen bij algemene maatregel van bestuur worden verplicht een open standaard toe te passen. Een standaard kan worden aangewezen als dat noodzakelijk en proportioneel is voor de werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van het elektronische verkeer met of tussen overheidsorganisaties of als dat voortvloeit uit internationale verplichtingen.
6	Voor diensten een is een betrouwbaarheidsniveau vastgesteld <sup>14</sup>	Wet digitale overheid (nog niet in werking)	Op basis van de (voorgestelde) Wet digitale overheid zullen overheidsorganisaties verplicht worden voor hun elektronische diensten waarvoor veilige toegang nodig is, het betrouwbaarheidsniveau substantieel of hoog te gebruiken. Bij het zullen dienstverleners zich moeten houden aan nader Uitvoeringsregelgeving zal kaders bieden voor het bepalen van het bij de dienstverlening passende betrouwbaarheidsniveau.
7	Goedgekeurde identificatie- en authenticatiemiddelen worden geaccepteerd <sup>15</sup>	Wet digitale overheid (nog niet in werking)	Vanuit het belang van het faciliteren van burgers en bedrijven en het belang van een veilige en betrouwbare identificatie- en authenticatieketen, verplicht dit wetsvoorstel overheidsorganisaties om bij elektronische dienstverlening de toegelaten identificatiemiddelen, erkende middelen en de bij de Europese Commissie genotificeerde middelen te accepteren, voor zover die middelen minimaal het voor de af te nemen dienst vereiste betrouwbaarheidsniveau ondersteunen.

<sup>12</sup> Artikel 3 Archiefwet 1995

<sup>13</sup> <https://www.digitaleoverheid.nl/document/memorie-van-toelichting-wet-digitale-overheid/>, p. 5-6

<sup>14</sup> <https://www.digitaleoverheid.nl/document/memorie-van-toelichting-wet-digitale-overheid/>, p. 12-13.

<sup>15</sup> <https://www.digitaleoverheid.nl/document/memorie-van-toelichting-wet-digitale-overheid/>, p. 14-15.

Nr.	Verplichting	Bron	Toelichting
8	Indiener ontvangt ontvangstbevestiging na indienen <sup>16</sup>	Wet modernisering elektronisch bestuurlijk verkeer	Wanneer een overheidsorganisatie via elektronische weg een formeel bericht ontvangt (zoals een aanvraag voor een product of dienst), verstuurt het een ontvangstbevestiging. Dit tenzij de verzender en het bestuursorgaan gebruikmaken van hetzelfde systeem van gegevensverwerking, en de verzender kan zien dat het bericht door de overheidsorganisatie ontvangen is. Bovendien hoeft geen ontvangstbevestiging te worden verzonden als de afzender geen elektronisch adres heeft opgegeven waarop hij te bereiken is. Het bestuursorgaan moet daar wel naar vragen in het formulier.
9	Inzage in ingevulde gegevens <sup>17</sup>	Wet modernisering elektronisch bestuurlijk verkeer	De overheidsorganisatie maakt door de indiener ingevulde gegevens aan die indiener beschikbaar. Deze inzagemogelijkheid dient beveiligd te zijn op een manier die passend is bij de vertrouwelijkheid en gevoeligheid van de verstrekte gegevens.
10	Verantwoording bij verzending en ontvangst berichten <sup>18</sup>	Wet modernisering elektronisch bestuurlijk verkeer	Indien overheidsorganisaties gebruik maken van een mijnomgeving of ander systeem waarin de burger of ondernemer toegang heeft tot door de overheid verzonden berichten, moet de overheidsorganisatie kunnen aantonen dat via dit systeem beschikbaar gestelde informatie is verzonden en (eventueel) ontvangen. Dit is geen verplichting om alles te loggen. De overheidsorganisatie kan zelf bepalen met welke gegevens in de meeste gevallen aan een bewijsplicht kan worden voldaan en het loggen beperken tot die gegevens.
11	Correctiegelegenheid na onjuiste indiening <sup>19</sup>	Wet modernisering elektronisch bestuurlijk verkeer	Na ontvangst van een niet via de aangegeven weg ingediend bericht kan worden volstaan met de mededeling dat het bericht onjuist is ingediend en het wijzen op de juiste manier van indienen. <sup>20</sup> In drie gevallen volstaat zo'n mededeling echter niet: <ol style="list-style-type: none"> <li>1. als het bericht zonder nadere bewerking kan worden behandeld</li> <li>2. als het bericht een bezwaarschrift of een administratief beroepschrift is, of</li> <li>3. als voor het bericht in kwestie geen wijze van indiening was aangewezen (dan kan de burger niet worden verweten dat hij een fout heeft gemaakt).</li> </ol>

<sup>16</sup> <https://www.digitaleoverheid.nl/document/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer-11-april-2017/>, p 7.

<sup>17</sup> <https://www.digitaleoverheid.nl/document/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer-11-april-2017/>, p 7-8.

<sup>18</sup> <https://www.digitaleoverheid.nl/document/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer-11-april-2017/>, p 8.

<sup>19</sup> <https://www.digitaleoverheid.nl/document/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer-11-april-2017/>, p 9.

<sup>20</sup> Maar dit is natuurlijk niet heel klantvriendelijk...

Nr.	Verplichting	Bron	Toelichting
12	Toegankelijkheid websites en apps <sup>21</sup>	Tijdelijk besluit digitale toegankelijkheid overheid en Wet digitale overheid (nog niet in werking)	Websites en mobiele apps van Nederlandse overheidsinstanties moeten voldoen aan de toegankelijkheidseisen volgens de Europese norm 301 549. Hierover moet verantwoording worden afgelegd in een toegankelijkheidsverklaring. Deze eisen gelden voor websites van overheidsorganisaties en mobiele applicaties.

## 6.2. Bouwblokken digitale overheid

### 6.2.1. Mijn Overheid lopende zaken en federatief berichtenstelsel

Mijn Overheid Lopende Zaken dient hetzelfde doel als PDS: gebruikers de voortgang van een aanvraag stap voor stap laten volgen. Maar de techniek verschilt sterk: Mijn Overheid Lopende Zaken werkt op basis van StUF-zaakberichten. Deze moeten op basis van het Digikoppeling ebMS-koppelvak aangeleverd worden. Hierbij is beveiliging met dubbelzijdig TLS en een PKI-overheid-certificaat noodzakelijk.

Omdat het berichtenverkeer van MijnOverheid, de BerichtenBox app, MijnGegevens app en het (formele) berichtenverkeer aan inwoners en ondernemers gaat veranderen, is het waarschijnlijk beter om vooruit te kijken en te bepalen hoe PDS kan aansluiten bij ontwikkelingen rondom het Federatieve Berichtenstelsel (FBS). Dat heeft tot doel om de digitale dienstverlening te verbeteren, het beheer goedkoper te maken en de toepassingen uit te bereiden. Tijdens het ontwikkelingsproces van de referentiearchitectuur PDS is contact gelegd met een aantal bij de ontwikkeling van FBS betrokkenen, maar ontbrak de documentatie om nader uit te werken hoe de relatie met PDS eruit ziet.

### 6.2.2. Notificatieservices en gebeurtenisgedreven werken

Bij het aanvragen van een product en bij het behandelen van een productaanvraag bereikt het proces steeds een andere status. Een burger, bedrijf of instelling kan deze status zelf opvragen via verschillende kanalen.

Een ander patroon ontstaat als er een notificatie gestuurd wordt op basis van een gebeurtenis. Deze gebeurtenissen worden naar een centraal notificatierouteringscomponent gestuurd. Informatiesystemen kunnen zich abonneren op bepaalde gebeurtenissen. Op het moment dat er een gebeurtenis is opgetreden die relevant kan zijn voor een informatiesysteem, onderneemt dit informatiesysteem (op basis van regels) actie.

In het kader van PDS-informatie kan een specifiek interactiecomponent geabonneerd zijn op gebeurtenissen die te maken hebben met een productaanvraagstatus of zaakstatus. Zodra een status van een zaak door een processysteem wordt gewijzigd, wordt de interactiecomponent daarvan op de hoogte gesteld. Het interactiecomponent kan op basis van die notificatie de gewenste gegevens ophalen en tonen aan de gebruiker.

<sup>21</sup> <https://digitoegankelijk.nl/wetgeving/wat-verplicht>.



Door de projectgroep Notificatieservices wordt gewerkt aan een 'Nederlandse Notificatie Strategie' . Bij de ontwikkeling hiervan zijn overheidsorganisaties uit de verschillende bestuurslagen betrokken. Verder wordt nadrukkelijk aansluiting gezocht bij wereldwijd gebruikte standaarden, zoals de CloudEvents specificatie<sup>22</sup>. Naar verwachting leidt dit tot een RESTful API standaard die functioneel beschreven is en overheidsbreed toegepast kan worden.

Het toepassen van deze nieuwe standaard (in ontwikkeling) kan een meerwaarde bieden in de dienstverlening naar burgers, bedrijven en instellingen. Door opname van de referentiecomponent Notificatierouteringscomponent en bijhorende Notificaties API in de referentiearchitectuur PDS is reeds rekening gehouden met deze nieuwe standaard.

---

<sup>22</sup> <https://cloudevents.io/>

## 7.Principes

Architectuurprincipes, afgeleid van principes uit de NORA, GEMMA, GEMMA Gegevenslandschap en de GEMMA referentiearchitectuur Omnichannel.

### 7.1. Architectuurprincipes PDS

PDS-principe 1	PDS-informatie is aangepast op de behoefte van de ontvanger
Rationale	PDS-informatie informeert de ontvanger zo goed mogelijk over de status van levering van een product of dienst. Dit vereist dat de getoonde informatie op de behoeften van die ontvanger is afgestemd.
Implicaties voor referentiearchitectuur PDS	De referentiearchitectuur PDS beschrijft het aanbieden van gegevens als PDS-informatie voor verschillende doelgroepen.
Implicaties voor implementaties PDS	<p>Implementaties van PDS worden zodanig ingericht dat inhoud, taalgebruik en presentatie van PDS-informatie worden aangepast aan de ontvanger. Deze informatie is voor die ontvanger:</p> <ul style="list-style-type: none"> <li>• actueel;</li> <li>• begrijpelijk, en</li> <li>• compleet.</li> </ul> <p>Dit betekent dat niet in alle gevallen dezelfde gegevens als PDS-informatie worden aangeboden. Een burger zal bijvoorbeeld een ander(e) kennisniveau en informatiebehoefte hebben dan een klantenservicemedewerker van een overheidsorganisatie.</p>
Bronprincipe(s)	<p>Dit principe is afgeleid van:</p> <ul style="list-style-type: none"> <li>• <a href="#">Afnemers krijgen de dienstverlening waar ze behoefte aan hebben (NORA).</a></li> <li>• <a href="#">Afnemers krijgen gerelateerde diensten gebundeld aangeboden (NORA).</a></li> <li>• <a href="#">Afnemers hebben inzage in voor hen relevante informatie (NORA).</a></li> <li>• <a href="#">Onze gemeente biedt de klant een goede informatiepositie (GEMMA).</a></li> <li>• <a href="#">Onze gemeente denkt vanuit de positie van de klant (GEMMA).</a></li> <li>• <a href="#">Serviceformules zijn leidend voor de inrichting van omnichannel-dienstverlening (GEMMA referentiearchitectuur Omnichannel).</a></li> <li>• <a href="#">De gemeente heeft integraal zicht op de situatie van de klant (GEMMA referentiearchitectuur Omnichannel).</a></li> </ul>

PDS-principe 2	PDS-informatie kan via meerdere kanalen worden ontvangen
Rationale	Niet iedere ontvanger wil op dezelfde manier PDS-informatie ontvangen. PDS-informatie kan daarom via meerdere kanalen worden aangeboden.
Implicaties voor referentiearchitectuur PDS	De referentiearchitectuur PDS beschrijft hoe PDS-informatie kan worden aangeboden, ongeacht het kanaal dat daarvoor wordt gebruikt.
Implicaties voor implementaties PDS	Implementaties van PDS worden zodanig ingericht dat PDS-informatie (op termijn) via meerdere kanalen kan worden aangeboden.
Bronprincipe(s)	<p>Dit principe is afgeleid van:</p> <ul style="list-style-type: none"> <li>• <a href="#">Afnemers hebben eenvoudig toegang tot de dienst (NORA).</a></li> </ul>

<b>PDS-principe 3</b>		<b>PDS-informatie werkt op basis van (bestaande) componenten en standaarden</b>
Rationale		De drempel om PDS-informatie aan te bieden moet laag zijn. Daarom wordt gebruikgemaakt van componenten met helder gedefinieerde verantwoordelijkheden en reeds beschikbare open standaarden. PDS kan zo 'meegroeien' met de ontwikkeling van standaarden en het beschikbaar komen van oplossingen van leveranciers die PDS-informatie bijvoorbeeld via een nieuw kanaal beschikbaar maken.
Implicaties voor referentiearchitectuur PDS		De referentiearchitectuur maakt waar mogelijk (her)gebruik van open standaarden die los installeerbare componenten verbinden.
Implicaties voor implementaties PDS		Implementaties van PDS gebruiken de in de referentiearchitectuur beschreven standaarden en componenten en maken bij de presentatie van PDS-informatie gebruik van standaardoplossingen als NL Design System.
Bronprincipe(s)		<p>Dit principe is afgeleid van:</p> <ul style="list-style-type: none"> <li>• <a href="#">Afnemers ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen (NORA).</a></li> <li>• <a href="#">Onze gemeente gebruikt generieke processen en functies (GEMMA).</a></li> <li>• <a href="#">COMPONENTGEBASEERD – We werken met ontkoppelde componenten (GEMMA Gegevenslandschap).</a></li> <li>• <a href="#">STANDAARD – We standaardiseren maximaal (GEMMA Gegevenslandschap).</a></li> <li>• <a href="#">Applicatiecomponenten voor kanalen en klantinteractie bevatten geen proceslogica (GEMMA referentiearchitectuur Omnichannel).</a></li> </ul>

<b>PDS-principe 4</b>		<b>PDS-informatie komt uit de bron</b>
Rationale		Het is belangrijk dat PDS-informatie actueel en juist is. PDS informatie wordt daarom (voor zover mogelijk) op aanvraag verstrekt en bij de bron verkregen.
Implicaties voor referentiearchitectuur PDS		De referentiearchitectuur beschrijft interactiepatronen om op basis van notificaties over statusveranderingen gegevens die onderdeel (kunnen) zijn van PDS-informatie vanuit de bijbehorende bronregistraties op te halen en aan de ontvanger aan te bieden.
Implicaties voor implementaties PDS		Implementaties van PDS volgen (voor zover mogelijk) de in de referentiearchitectuur beschreven interactiepatronen
Bronprincipe(s)		<p>Dit principe is afgeleid van:</p> <ul style="list-style-type: none"> <li>• <a href="#">Afnemers kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt (NORA).</a></li> <li>• <a href="#">Onze gemeente hergebruikt gegevens (GEMMA).</a></li> <li>• <a href="#">EENMALIGE VASTLEGGING – We leggen gegevens eenmalig vast en vragen op bij de bron (GEMMA Gegevenslandschap).</a></li> <li>• <a href="#">De gemeente garandeert een consistent resultaat ongeacht het gebruikte kanaal (GEMMA referentiearchitectuur Omnichannel).</a></li> </ul>

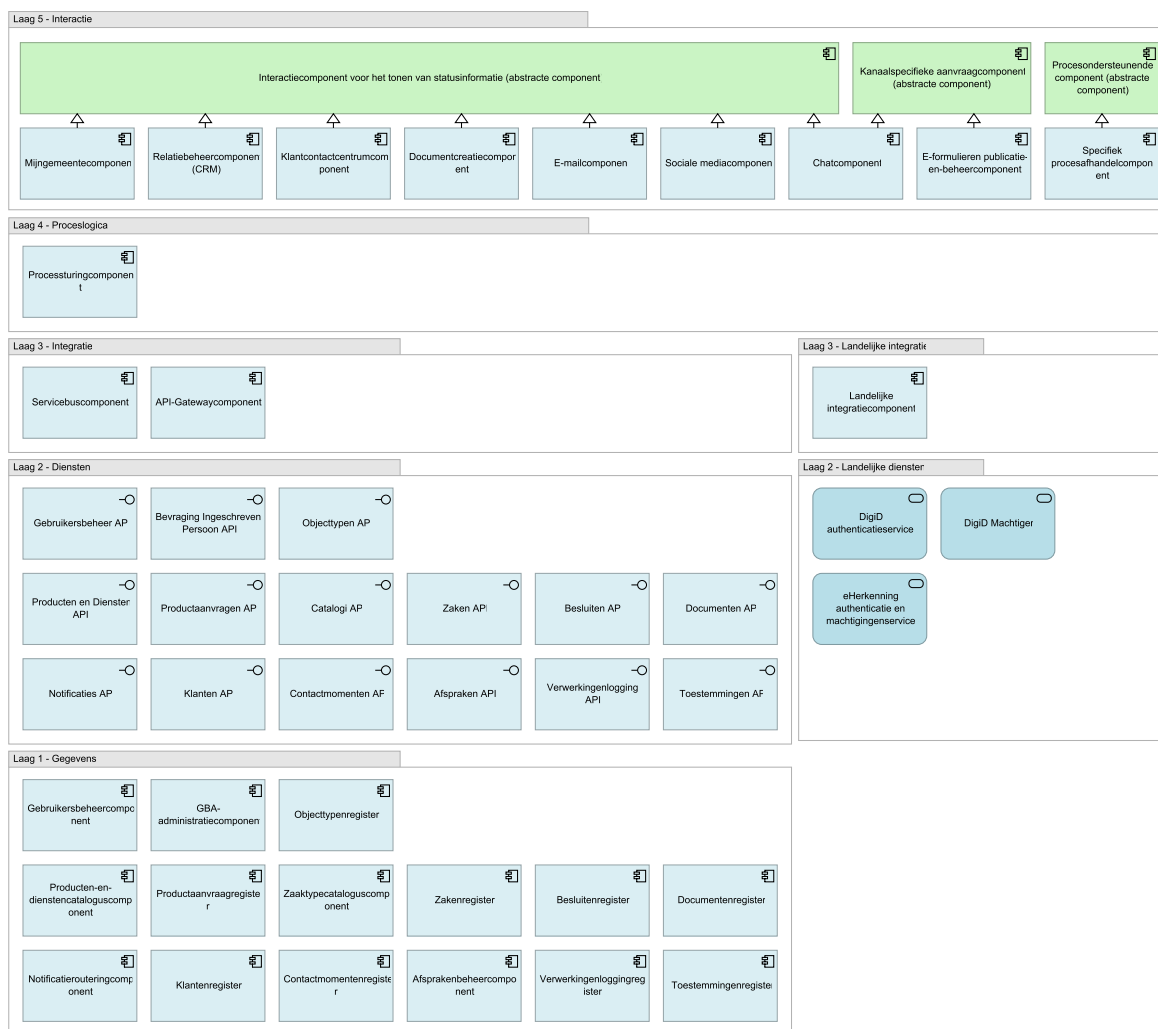
<b>PDS-principe 5</b>		<b>PDS-informatie wordt vertrouwelijk verwerkt</b>
Rationale		PDS-informatie omvat persoonsgegevens en mogelijk andere gevoelige data die bijvoorbeeld te maken hebben met de financiële situatie van de aanvrager. Deze gegevens worden vertrouwelijk, en in lijn met wet- en regelgeving behandeld.

PDS-principe 5	PDS-informatie wordt vertrouwelijk verwerkt
Implicaties voor <i>referentiearchitectuur PDS</i>	De referentiearchitectuur beschrijft hoe toegang tot gegevens wordt beperkt voor ontvangers die daartoe niet gerechtigd zijn, en licht toe hoe deze gegevens conform relevante wet- en regelgeving verwerkt moeten worden.
Implicaties voor <i>implementaties PDS</i>	Implementaties van PDS beperken de toegang tot PDS-informatie, verwerken die volgens relevante wet- en regelgeving en bieden burgers inzage in het gebruik van PDS-informatie door medewerkers van de gemeente.
Bronprincipe(s)	Dit principe is afgeleid van: <ul style="list-style-type: none"> <li>• <a href="#">Afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt (NORA).</a></li> <li>• <a href="#">Onze gemeente gaat op een vertrouwelijke manier met gegevens om (GEMMA).</a></li> <li>• <a href="#">VERTROUWD – We zorgen dat informatiebeveiliging en privacy op orde zijn (GEMMA Gegevenslandschap).</a></li> <li>• <a href="#">REGIE OP GEGEVENS – We faciliteren regie op gegevens (GEMMA Gegevenslandschap).</a></li> </ul>

## 8. Bijlagen

### 8.1. Overzicht generieke PDS componenten

Onderstaande afbeelding toont de generieke componenten en API's die betrokken (kunnen) zijn bij het ontstaan of tonen van PDS-informatie. Het betreft hier een verzameling van de componenten die voor de verschillende casussen benodigd kunnen zijn.



Figuur 18: Overzicht generieke componenten

Om generieke interactiepatronen te kunnen vormgeven, toont bovenstaand model drie abstracte componenten, die hieronder nader worden toegelicht. Een nadere beschrijving van de meeste andere opgenomen componenten is te vinden op GEMMA Online.<sup>23</sup>

<sup>23</sup> [https://www.gemmaonline.nl/index.php/Overzicht\\_allereferentiecomponenten](https://www.gemmaonline.nl/index.php/Overzicht_allereferentiecomponenten)

Component	Beschrijving
Interactiecomponent voor het tonen van statusinformatie	De interactiecomponent voor het tonen van statusinformatie wordt gebruikt om via een specifiek kanaal statusinformatie bij lopende aanvragen van producten of diensten aan een burger, (vertegenwoordiger van een) bedrijf of medewerker te tonen. De interactiecomponent voor het tonen van statusinformatie is een abstract component. Dat betekent dat verschillende concrete componenten (zoals een Mijngemeentecomponent) de functies die horen bij de interactiecomponent voor het tonen van statusinformatie kunnen vervullen.
Kanaalspecifieke aanvraagcomponent	De kanaalspecifieke aanvraagcomponent ondersteunt het aanvragen van producten of diensten bij de gemeente via één of meerdere specifieke kanalen. De kanaalspecifieke aanvraagcomponent is een abstract component. Dat betekent dat verschillende concrete componenten (zoals een E-formulieren publicatie-en-beheercomponent) de functies die horen bij de Kanaalspecifieke aanvraagcomponent kunnen vervullen.
Procesondersteunende component	Abstract verzamelcomponent voor procesondersteunende systemen die zaakgericht zijn ingericht.

## 8.2. Casus MijnGemeente

*Deze casus is beschreven voor gemeenten.*

Burgers, bedrijven of instellingen die producten van de overheid afnemen, weten vaak niet (goed genoeg) wat de status van hun productaanvraag is of hoe lang het nog gaat duren voordat het product geleverd wordt. Het komt voor dat ze met meerdere organisaties contact moeten opnemen om dit te achterhalen – het bekende van het kastje naar de muur sturen. Met PDS kunnen burgers en bedrijven de levering van producten en diensten volgen, ook als daarbij meerdere overheidsorganisaties betrokken zijn. Zij worden proactief en via een kanaal naar keuze geïnformeerd over die levering.

Een aantal gemeenten gaat in 2021 een MijnGemeente-omgeving implementeren ter ondersteuning van de dienstverlening aan burgers en bedrijven. De basis hiervoor is het Integraal Klantbeeld, waarvan PDS-informatie een onderdeel is. De scope van deze casus is groot genoeg om aan te kunnen tonen dat de uitgewerkte architectuur toegepast kan worden om burgers en ondernemers via een webportaal te informeren, en klein genoeg om de benodigde software en processen middels een beperkt aantal componenten in beperkte tijd te implementeren.

### 8.2.1. Casusbeschrijving

Een inwoner wil op een persoonlijke pagina van een gemeente (MijnGemeente portaal) een overzicht van relevante klantgegevens in samenhang zien. Hierbij worden alleen die gegevens getoond waartoe de inwoner geautoriseerd is. Het opvragen van de gegevens wordt vastgelegd ter verantwoording aan de inwoner. Wij denken op dit moment dat hiervoor onderstaande gegevens nodig zijn. De dikgedrukte gegevens zijn de gegevens waarop we ons in het PDS-traject met name richten.

- Naam- en contactgegevens
- Klantvoorkeuren
- Aangevraagde en geleverde producten
  - Geleverde producten
  - **Lopende aanvragen inclusief status**
  - Bij aanvragen geleverde documenten
- Zaken
  - Afgeronde zaken
  - **Lopende zaken inclusief inzage in status en behandelaar**
  - Documenten bij een zaak
  - Besluiten genomen bij een zaak
- Contactmomenten
  - Gevoerde contacten
  - Toekomstige afspraken
- Verwerkingenlogging-gegevens

### 8.3. Casus CRM

*Deze casus is beschreven voor gemeenten.*

Een goed geïnformeerde burger staat minder vaak aan de balie. En doordat overheidsorganisaties op een eenduidige manier informatie met elkaar delen, kunnen vragen worden beantwoord door een klantenservicemedewerker in plaats van de vakspecialist. Zij hebben daardoor meer tijd voor het leveren van goede dienstverlening en ondersteuning op maat. PDS-informatie kan daarnaast worden gebruikt voor het bewaken van het verloop van (keten)processen en het bijsturen van de inrichting daarvan.

Een aantal organisaties gaat een CRM-platform implementeren. De basis hiervoor is het Integraal Klantbeeld, waarvan PDS-informatie een onderdeel is. De scope van deze casus is groot genoeg om aan te kunnen tonen dat de uitgewerkte architectuur toegepast kan worden om KCC-medewerkers te ondersteunen bij het informeren van burgers en ondernemers, en klein genoeg om de benodigde software en processen middels een beperkt aantal componenten in beperkte tijd te implementeren.

#### 8.3.1. Casusbeschrijving

Een medewerker van de gemeente wil inwoners goed voor kunnen lichten. Daarvoor is het nodig dat het CRM-platform een overzicht van relevante klantgegevens in samenhang toont. Hierbij worden alleen die gegevens getoond waartoe de medewerker geautoriseerd is. Het opvragen van de gegevens wordt vastgelegd ter verantwoording aan de inwoner. Wij denken op dit moment dat hiervoor onderstaande gegevens nodig zijn. De dikgedrukte gegevens zijn de gegevens waarop we ons in het PDS-traject met name richten.

- Naam- en contactgegevens
- Klantvoorkeuren
- Aangevraagde en geleverde producten
  - Geleverde producten
  - **Lopende aanvragen inclusief status**
  - Bij aanvragen geleverde documenten
- Zaken
  - Afgeronde zaken
  - **Lopende zaken inclusief inzage in status en behandelaar**
  - Documenten bij een zaak
  - Besluiten genomen bij een zaak
- Contactmomenten
  - Gevoerde contacten
  - Toekomstige afspraken



## 8.4. Statusuitwisseling tussen organisaties

Behandelaars van zaken waarvan de behandeling (deels) is uitbesteed aan externe organisaties hebben inzicht nodig in de voortgang van die behandeling door die externe organisaties. Bovendien komt het voor dat burgers, bedrijven of instellingen met meerdere organisaties contact moeten opnemen om te achterhalen hoe het er met hun aanvraag van een product of dienst voorstaat – het bekende van het kastje naar de muur sturen. Met PDS kunnen medewerkers van overheidsorganisaties, burgers en bedrijven de levering van producten en diensten volgen, ook als daarbij meerdere overheidsorganisaties betrokken zijn. Zij worden proactief en via een kanaal naar keuze geïnformeerd over die levering.

Een aantal organisaties gaat een beperkte omgeving implementeren. De basis hiervoor is het Integraal Klantbeeld, waarvan PDS-informatie een onderdeel is. De scope van deze casus is groot genoeg om aan te kunnen tonen dat de uitgewerkte architectuur over meerdere organisaties heen toegepast kan worden, en klein genoeg om de benodigde software en processen middels een beperkt aantal componenten in beperkte tijd te implementeren.

### 8.4.1. Casusbeschrijving

Twee overheidsorganisaties zijn betrokken bij de levering van één product of dienst aan een burger of ondernemer. Bij de eerste organisatie (de leverancier) wordt door een burger een product aangevraagd waarvoor een deelproduct van een tweede organisatie (de onderaannemer) aan de leverancier geleverd wordt.

De leverancier bestelt dit deelproduct bij de tweede organisatie. De onderaannemer geeft een notificatie aan de eerste organisatie door als een behandelstatus voor het deelproduct is veranderd. Op basis daarvan kan de leverancier de status van de behandeling van het deelproduct bij de onderaannemer opvragen. Voor deze casus denken wij dat de tenminste onderstaande gegevens nodig zijn:

- Producten
  - Overzicht te leveren producten door organisaties aan elkaar
- Aangevraagde en geleverde producten
  - **Lopende aanvragen inclusief status**
  - Bij aanvragen geleverde documenten
- Zaken (gestart door de onderaannemer naar aanleiding van aanvraag door leverancier)
  - **Lopende zaken inclusief inzage in status en behandelaar**
  - Documenten bij een zaak
  - Besluiten genomen bij een zaak